(19) **RU** (11) **99121839** (13) **A**

(51) 7 H04N7/16

FEDERAL SERVICE
UNDER THE INTELLECTUAL
PROPERTY,
PATENTS AND TRADE MARKS
(ROSPATENT)

(12) APPLICATION FOR INVENTION

(14) Document date: **2001.08.27**
(21) Application number: **99121839/09**
(22) Application filing date: **1998.03.19**
(31) Priority application number: **97400650.4**
(32) Date of filing of priority application: **1997.03.21**
(33) Alloting country or organization: **EP**
(31) Priority application number: **PCT/EP97/02106**
(32) Date of filing of priority application: **1997.04.25**
(33) Alloting country or organization: **WO**
(31) Priority application number: **97402959.7**
(32) Date of filing of priority application: **1997.12.05**
(33) Alloting country or organization: **EP**
(43) Unexamined printed documents without grant: **2001.08.27**
(71) Applicant information: **КАНАЛЬ+СОСЬЕТЭ АНОНИМ (FR)**
(72) Inventor information: **МАЙЯР Мишель (FR)**
(74) Attorney, agent, representative information: **Поликарпов Александр Викторович**
(85) PCT date art. 22/39: **1999.10.21**
(86) PCT or regional filing information: **EP 98/01606 (19.03.1998)**
(87) PCT or regional filing information (publ.): **WO 98/43428 (01.10.1998)**
(98) Mail address: **193036, Санкт-Петербург, а/я 24, "Невинпат", Поликарпову А.В.**

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМЕ УСЛОВНОГО ДОСТУПА

1. Способ предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, включающий операцию программирования приемника/декодера таким образом, что прием текущего EMM текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее EMM предыдущего календарного периода.

2. Способ по п.1, дополнительно включающий следующие операции: передача с текущим EMM избыточной информации о дате, и прием текущего EMM и использование избыточной информации о дате для проверки факта приема упомянутого предыдущего EMM.

3. Способ по п.2, в котором каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, и соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, причем указанная информация о контрольной дате представляет собой указанную избыточную информацию о дате.

4. Способ по п.2 или 3, в котором избыточная информация о дате представляет собой ключ сообщения

управления правами (ключ ECM) предыдущего календарного периода.

5. Способ по пп.2-4, в котором права подписчика изменяются через регулярные промежутки времени, и избыточная информация о дате относится к непосредственно предшествующему периоду.

6. Способ по любому из предшествующих пунктов, в котором календарные периоды не являются смежными во времени и/или эти периоды разделены нестандартизированными интервалами времени.

7. Способ по любому из предшествующих пунктов, в котором текущее EMM содержит битовый массив подписки, позиции которого представляют права подписки подписчиков в группе, факультативно, только при изменении прав подписчика.

8. Передатчик для использования в способе предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, которым предусмотрено программирование приемника/декодера таким образом, что прием текущего EMM текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее EMM предыдущего календарного периода, где указанный передатчик содержит средства передачи с текущим EMM текущего календарного периода избыточной информации о дате, которая может быть использована приемником/декодером для проверки факта приема упомянутого предыдущего EMM.

9. Передатчик по п.8, в котором каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой указанную избыточную информацию о дате.

10. Передатчик по п. 8 или 9, в котором избыточная информация о дате представляет собой ключ сообщения управления правами (ключ ECM) предыдущего календарного периода.

11. Приемник/декодер для использования в способе предотвращения несанкционированного доступа в системе условного доступа, который подключен к системе условного доступа и выполнен с возможностью приема сообщения управления предоставлением прав (EMM) для группы подписчиков для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, содержащий средство, запрограммированное таким образом, чтобы осуществлять прием текущего EMM текущего календарного периода только в том случае, когда им было принято по меньшей мере одно предыдущее EMM предыдущего календарного периода.

12. Приемник/декодер по п.11, в котором упомянутые средства запрограммированы для выполнения проверки факта приема предыдущего EMM, используя избыточную информацию о дате, содержащуюся в текущем EMM.

13. Приемник/декодер по п.12, в котором каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой указанную избыточную информацию о дате.

14. Приемник/декодер по п.12 или 13, в котором избыточная информация о дате представляет собой ключ сообщения управления правами (ключ ECM) предыдущего календарного периода.

Перевод
с английского

Конвенционная заявка
на патент с приоритетом
от 21 марта 1997 г.,
25 апреля 1997 г. и 5 декабря 1997 г.
на имя инофирмы
КАНАЛЬ+ СОСЬЕТЭ АНОНИМ, Франция
PCT/EP98/01606

СПОСОБ И УСТРОЙСТВО ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМЕ УСЛОВНОГО ДОСТУПА

Предлагаемое изобретение относится к способу и устройству для предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика. Способ может быть использован в области передачи данных, когда передаваемые зашифрованные данные принимаются и расшифровываются, например, приемником/декодером санкционированного пользователя.

Термин "приемник/декодер", используемый здесь, может подразумевать приемник для приема либо закодированных, либо незакодированных сигналов, например, теле- и /или радиосигналов. Термин может также подразумевать декодер для декодирования принимаемых сигналов. Реализации таких приемников/декодеров могут включать декодер, интегрированный с приемником

для декодирования принимаемых сигналов, например, в компьютерной приставке к телевизору, или декодер, работающий в сочетании с приемником, выполненным физически отдельно.

Упомянутый выше приемник/декодер "подключен к" системе условного доступа, что предполагает возможность того, что приемник/декодер является либо составной частью системы условного доступа, либо отдельным устройством.

В частности, но не исключительно, изобретение может использоваться в системе вещания, ориентированной на массовый рынок, имеющей некоторые или все из следующих предпочтительных характеристик. Так, это может быть система вещания информации, предпочтительно система радио и/или телевизионного вещания; спутниковая система (хотя возможно использование для кабельной или наземной трансляции); цифровая система, предпочтительно использующая систему сжатия MPEG, более предпочтительно MPEG-2, при трансляции данных/сигналов; она может допускать возможность интерактивной работы; и она использует смарт-карты. Опять-таки, данное изобретение может использоваться в сочетании с цифровыми аудиовизуальными системами трансляции. В контексте данного изобретения термин "цифровая аудиовизуальная система трансляции" относится ко всем системам трансляции для трансляции или вещания в первую очередь аудиовизуальных или мультимедийных цифровых данных. Хотя данное изобретение наиболее применимо к цифровым телевизионным системам вещания, данное изобретение может в равной степени использоваться для фильтрации данных, рассылаемых фиксированной телекоммуникационной сетью для мультимедийных Интернет-приложений и т.д.

Используемый здесь термин "смарт-карта" включает (но не исключительно) любое устройство в виде карты на основе микросхемы,

содержащее, например, микропроцессор и/или запоминающее устройство. Этот термин включает также устройства на основе микросхем, имеющие иные геометрические формы, например, устройства в форме ключа, которые часто используются в системах ТВ декодеров.

Термин MPEG определяет стандарты передачи данных, разработанные рабочей группой "Motion Pictures Expert Group" (экспертная группа по движущимся изображениям) Международной организации по стандартизации, и, в частности, но не исключительно, стандарт MPEG-2, разработанный для цифровых телевизионных приложений и утвержденный в документах ISO 13818-1, ISO 13818-2, ISO 13818-3, и ISO 13818-4. В контексте данной патентной заявки этот термин включает все варианты, модификации или разработки форматов MPEG, применимые в области передачи цифровых данных.

Целью данного изобретения является предоставить способ передачи данных, передатчик и приемник/декодер, которые могут использоваться для предоставления данных, например, подписчикам, или другим покупателям права на прием, в защищенном режиме.

В существующих системах вещания смарт-карта используется подписчиком для получения права на прием, и, как было установлено в соответствии с настоящим изобретением, существует проблема предотвращения некорректного использования карты с целью обмана обладателя прав.

Например, в известной системе подписчиков MPEG телевидения права различных подписчиков или групп подписчиков можно проверять централизованно, например, ежемесячно, и затем с центральной станции рассылать сообщение санкционирования каждому подписчику или группе подписчиков для санкционирования (или блокирования) использования этих прав. Для удобства сообщение санкционирования представляет собой просто "1"

или "0", расположенные в различных позициях битового массива, которые назначаются соответствующим подписчикам для данного месяца, причем только наличие "1" санкционирует использование указанного права подписчиком, соответствующим данной позиции битового массива, а "0" запрещает использование прав.

В данной системе возникает следующая проблема, решаемая в соответствии с предлагаемым изобретением. Если, например, первоначальный подписчик прекращает оплату прав, по истечении некоторого промежутка времени система не будет более идентифицировать указанного первоначального подписчика ранее назначенной позицией битового массива, и эта позиция может затем вновь быть назначена для идентифицирования "нового" подписчика. Если указанный новый подписчик заплатил за использование прав, и, следовательно, использование этих прав ему было санкционировано, в той же позиции битового массива опять установится "1". Если в приемнике/декодере "первоначального" подписчика декодер отключается до того, как следующее сообщение санкционирования может обновить подключенную к нему систему условного доступа (ассоциированную с "первоначальным подписчиком"), и если декодер затем включается (или если часы переустанавливаются), "первоначальный" подписчик тогда будет принят за "нового" подписчика, которому было санкционировано использование прав, и "первоначальный" подписчик таким образом получит право обманным путем.

Предлагаемое изобретение предназначено для решения этой проблемы, а также подобных и связанных с ней других проблем, в случае, когда права подписчика могут предоставляться на периоды времени, которые могут обычно зависеть (но не исключительно) от оплаты счетов. Например, права могут предоставляться по соображениям, отличным от оплаты, когда различным

пользователям может быть санкционировано использование системы для получения доступа к защищенной области, защищенной информации или к некоторым другим защищенным услугам.

В контексте предлагаемого изобретения используются термины "EMM" и "ECM".

Сообщение управления предоставлением прав, или EMM (Entitlement Management Message), – это сообщение, предназначенное для одного подписчика или группы подписчиков. Оно обычно генерируется системой санкционирования доступа и мультиплексируется с потоком данных MPEG-2. Обычно оно зашифровывается с помощью так называемого ключа "управления", например, для использования группой. Следовательно, оно может быть зашифровано с помощью ключа, общего для всех подписчиков из одной группы подписчиков.

Сообщение управления правами или ECM (Entitlement Control Message) – это сообщение, посылаемое с одной скремблированной программой. ECM разрешает пользователю дескремблировать слово управления для получения права дескремблировать телевизионную (или подобную) программу. Ключ (в используемых терминах "ключ ECM") передается с помощью EMM подписчику, поскольку смарт-карта, используемая подписчиком, нуждается в ключе ECM для дешифровки ECM. Дешифрованное ECM используется для дескремблирования слова управления и, затем, для дескремблирования программы.

В соответствии с первым аспектом предлагаемого изобретения предлагается способ предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности

предоставлять доступ соответствующему подписчику, включающий операцию программирования приемника/декодера таким образом, что прием текущего ЕММ текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее ЕММ предыдущего календарного периода.

Таким образом, проблема предотвращения несанкционированного доступа будет решена.

Предпочтительно, чтобы способ содержал дополнительно следующие шаги:

передача избыточной информации о дате с текущим ЕММ, и

прием текущего ЕММ и использование избыточной информации о дате для проверки факта приема упомянутого предыдущего ЕММ.

В первом предпочтительном варианте реализации каждое ЕММ содержит информацию о дате прав, касающуюся текущего права доступа, и соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, причем указанная информация о контрольной дате представляет собой указанную избыточную информацию о дате. Этот вариант может оказаться особенно эффективным вариантом реализации изобретения на практике.

Во втором предпочтительном варианте реализации избыточная информация о дате представляет собой ключ ECM предыдущего календарного периода. Этот способ является удобным альтернативным вариантом представления такой информации.

Права подписчика могут изменяться через регулярные промежутки времени, и избыточная информация о дате может относиться к непосредственно предшествующему периоду.

В иллюстративном примере изобретения, где приемник/декодер является одним из множества приемников/декодеров системы вещания, подписчики

должны платить за текущий месяц за право приема программы или программ, и права подписчиков могут изменяться помесячно (поскольку некоторые могут не заплатить). Для индикации прав на текущий месяц может использоваться битовый массив. В этом случае, когда текущее EMM принимается декодером, избыточная информация о дате, например, "предыдущий" ключ ECM, будет относиться к непосредственно предшествующему месяцу. В то же время периоды времени не обязательно должны быть последовательными, поскольку "текущий" и "предыдущий" периоды могут быть не смежными во времени, и между ними могут быть промежутки времени нестандартизированной длины. Тем не менее, обычно предыдущее EMM предназначено для непосредственно предшествующего календарного периода, и периоды являются последовательными.

Когда происходят изменения прав подписчика, предпочтительно включить в текущее EMM битовый массив подписки, содержащий позиции, представляющие права подписки подписчиков из данной группы. Однако в этом нет необходимости в ситуациях, когда все подписчики санкционированы, например, если все подписчики оплатили свои подписки за соответствующий календарный период; следовательно, включение в текущее EMM битового массив подписки может выполняться только тогда, когда в правах подписчиков произошли изменения.

Согласно другому аспекту изобретения предлагается передатчик для использования в способе предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, которым предусмотрено

программирование приемника/декодера таким образом, что прием текущего EMM текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее EMM предыдущего календарного периода, где указанный передатчик содержит средства передачи с текущим EMM текущего календарного периода избыточной информации о дате, которая может быть использована приемником/декодером для проверки факта приема упомянутого предыдущего EMM.

Предпочтительно каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой избыточную информацию о дате. Как альтернатива, избыточная информация о дате может быть ключом ECM предыдущего календарного периода.

Согласно еще одному аспекту изобретения, предлагается приемник/декодер для использования в способе предотвращения несанкционированного доступа в системе условного доступа, который подключен к системе условного доступа и выполнен с возможностью приема сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, содержащий:

средства, запрограммированные таким образом, чтобы осуществлять прием текущего EMM текущего календарного периода только в том случае, когда ими было принято по меньшей мере одно предыдущее EMM предыдущего календарного периода

Упомянутые средства могут быть запрограммированы для выполнения проверки факта приема предыдущего EMM, используя избыточную информацию

о дате, содержащуюся в текущем EMM.

Каждое EMM может содержать информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой избыточную информацию о дате. Как альтернатива, избыточная информация о дате может быть ключом ECM предыдущего календарного периода.

Изобретением также предлагается приемник/декодер, в существенной степени как описанный здесь, со ссылками на прилагаемые фигуры и иллюстрированный ими.

Хотя предпочтительные варианты реализации изобретения относятся к системе спутникового телевидения, изобретение применимо к другим сетям передачи данных, включая кабельные сети (не обязательно обрабатывающие телевизионные сигналы).

Предпочтительные особенности изобретения описываются ниже на примере со ссылками на прилагаемые рисунки, среди которых:

Фиг. 1 иллюстрирует общую архитектуру системы цифрового телевидения;

Фиг. 2 иллюстрирует общую структуру смарт-карты;

Фиг. 3 иллюстрирует структуру сообщения управления предоставлением права (EMM), используемого в системе условного доступа;

Фиг. 4 иллюстрирует структуру сообщения EMM, зашифрованного с помощью группового ключа управления Kg, общего для всех подписчиков в группе, и предоставлена для иллюстрации проблемы, имеющей место в существующих системах;

На фиг. 5 показана часть структуры зашифрованного EMM в соответствии с настоящим изобретением;

Фиг. 6 иллюстрирует первый предпочтительный вариант реализации;

Фиг. 7 представляет собой блок-схему, иллюстрирующую первый предпочтительный вариант реализации;

Фиг. 8 иллюстрирует еще один предпочтительный вариант реализации.

На фиг. 1 приведена структура цифровой системы вещания и приема 1000, включающая обычную систему цифрового телевидения 2000, которая использует известную систему сжатия MPEG-2 для передачи сжатых цифровых сигналов. Устройство сжатия MPEG-2 2002 в центре вещания принимает поток цифровых сигналов (обычно поток видеосигналов). Устройство сжатия подключается к мультиплексору и скремблеру 2004 с помощью канала 2006. Мультиплексор 2004 принимает множество входных сигналов, собирает один или несколько несущих потоков и передает сжатые цифровые сигналы в передатчик 2008 центра вещания через канал 2010, тип которого, естественно, может быть различным, включая каналы телекоммуникаций. Передатчик 2008 передает электромагнитные сигналы через канал "земля-спутник" 2012 на спутниковый ретранслятор 2014, где выполняется их обработка электронными средствами и вещание через виртуальный канал "спутник-земля" 2016 на наземный приемник 2018, обычно имеющий форму тарелки, принадлежащий конечному пользователю или арендуемый им. Сигналы, принимаемые приемником/декодером 2018, передаются в совмещенный приемник/декодер 2020, принадлежащий конечному пользователю или арендуемый им и подключенный к телевизору 2022 конечного пользователя. Приемник/декодер 2020 декодирует сжатый MPEG-2 сигнал в телевизионный сигнал для телевизора 2022.

Система условного доступа 3000 (разрешающая доступ при выполнении некоторого условия) подключается к мультиплексору 2004 и приемнику/декодеру 2020 и располагается частично в центре вещания и частично в декодере. Она позволяет конечному пользователю осуществлять доступ к

вещательным передачам цифрового телевидения от одного или нескольких операторов вещания. В приемник/декодер 2020 может устанавливаться смарт-карта, которая может декодировать сообщения, относящиеся к коммерческим предложениям (т.е. одну или несколько телевизионных программ, продаваемых оператором вещания). С использованием декодера 2020 и смарт-карты пользователь может покупать передачи в режиме подписки или уплаты за просмотр (PPV – *Pay Per View*, уплата производится за каждую просмотренную передачу).

Система условного доступа 3000 включает систему санкционирования подписчиков (SAS). SAS подключается к одной или более системам управления подписчиками (SMS), одна SMS для каждого оператора вещания, посредством соответствующего канала TCP-IP (хотя вместо него могут использоваться альтернативные каналы других типов). В качестве альтернативы одна SMS может использоваться совместно двумя операторами вещания, или один оператор мог бы использовать две SMS и т.д.

Интерактивная система 4000, также подключенная к мультиплексору 2004 и приемнику/декодеру 2020, и также располагающаяся частично в центре вещания и частично в декодере, позволяет конечному пользователю взаимодействовать с различными приложениями через модемный обратный канал 4002.

Поскольку обычная конструкция и работа системы цифрового телевидения известна, ее дальнейшие подробности описываться не будут.

Дочерняя смарт-карта, или смарт-карта подписчика, схематически изображена на фиг. 2 и содержит 8-битовый микропроцессор 100, такой как микропроцессор Motorola 6805, имеющий шину ввода/вывода, подключенную к стандартному массиву контактов 102, которые при использовании подключаются

к соответствующему массиву контактов устройства считывания смарт-карты приемника/декодера 2020, имеющего обычную конфигурацию. Микропроцессор 100 соединен посредством шины с предпочтительно маскированным ПЗУ 104, ОЗУ 106 и электрически-стираемым программируемым ПЗУ 108. Смарт-карта соответствует стандартам ISO 7816-1, ISO 7816-2 и ISO 7816-3, которые определяют некоторые физические параметры смарт-карты, позиции контактов микросхемы и некоторые связи между внешней системой (и, в частности, приемником/декодером 2020) и смарт-картой соответственно, и поэтому далее описываться не будет. Одной из функций микропроцессора 100 является управление памятью смарт-карты.

Структура типового EMM представлена на фиг. 3. В общем, EMM, которое реализуется в виде последовательности битов цифровых данных, состоит из заголовка 3060, собственно EMM 3062 и подписи 3064. Заголовок 3060, в свою очередь, состоит из идентификатора типа 3066 для идентификации типа EMM – индивидуальный, групповой, зрительский или какой-либо другой, идентификатора размера 3068, который указывает размер EMM, необязательного адреса 3070 для EMM, идентификатора оператора 3072 и идентификатора ключа 3074. Собственно EMM, естественно, существенно различается в зависимости от его типа. И, наконец, подпись 3064, которая обычно имеет размер 8 байтов, содержит информацию для борьбы с искажениями остальных данных в EMM.

Предлагаемое изобретение в первую очередь связано со следующими предпосылками.

Предпосылки создания изобретения

В существующих системах вещания, использующих MPEG, для уменьшения требуемой пропускной способности, необходимой для пересылки ежемесячных сообщений санкционирования подписчиков (EMM), обычно

используются групповые ЕММ восстановления, зашифрованные с помощью группового ключа управления Kg, общего для всех подписчиков группы. Как показано на фиг. 4, собственно ЕММ содержит битовый массив подписчиков 3100, обычно из 256 битов. Каждый бит соответствует одному подписчику. В приведенном примере, бит №3 соответствует подписчику №3. Собственно ЕММ содержит также поле прав 3102, детализирующее подписные права для всех подписчиков из данной группы на этот месяц, а также содержит ключ ECM для данного месяца и, обычно, для следующего месяца. В предположении, что подписчик оплатил надлежащим образом свою подписку за январь, наличие 1 в данной позиции будет означать для декодера подписчика (после того, как он расшифровал сообщение с помощью ключа Kg), что подписчику действительно санкционирован прием программы в данной группе, как определено в поле прав подписчиков. Индивидуальные программы дескремблируются с использованием ECM, расшифрованного с помощью ключа ECM.

Если подписчик не внес необходимую плату за февраль, в битовом массиве в соответствующей позиции будет 0. После того, как смарт-карта в приемнике/декодере декодирует это сообщение, присутствие нуля в бите № 3 будет означать для декодера, что он уже не санкционирован на прием этих прав, и смарт-карта отметит это и предпримет соответствующие действия. На практике, инструкция удалить соответствующий ключ может быть переслана в отдельном ЕММ.

Вполне вероятно, что в марте в группу может быть добавлен новый подписчик. Это происходит довольно часто, поскольку группы подписчиков часто реорганизуются с целью уменьшения количества групп и числа сообщений ЕММ, которые необходимо пересылать. В этом случае, новому подписчику будет назначен бит № 3. Когда новый подписчик декодирует сообщение с помощью

ключа Kg, он обнаружит положительный бит 1 в этой позиции, указывающий, что ему санкционирован прием прав, соответствующих данной группе.

Оказалось, что описанную выше систему сравнительно легко обмануть. В данном случае подписчик №3 может просто отключить свой декодер в феврале. Если он это сделает, он не примет в феврале ни ЕММ, ни инструкцию для удаления соответствующего ключа.

Повторное включение декодера в марте позволит теперь уже несанкционированному декодеру декодировать ЕММ для марта, включая сообщение с положительным битом (предназначенное для нового подписчика) в бите № 3. Затем декодер придет к выводу, что он может продолжать получать права, соответствующие данной группе, и возникнет аномальная ситуация, в которой бит №3 группового сообщения будет предоставлять права двум декодерам, принадлежащим новому законному подписчику и предыдущему несанкционированному подписчику.

Предпочтительные варианты реализации изобретения

Данная проблема преодолевается путем передачи избыточной информации контрольной даты последовательно с каждым ЕММ, как показано в общем виде на фиг. 5. Каждый приемник/декодер 2020 программируется так, чтобы принимать ЕММ только в том случае, если он принял по крайней мере ЕММ предыдущего месяца. Поскольку права изменяются каждый месяц, необходимо просто сравнить текущие права, записанные в декодере (которые содержатся в секции текущих прав 3102), с предыдущими правами (которые содержатся в секции предыдущих прав 3104).

В первой предпочтительной реализации, которая описывается ниже более подробно с использованием фиг. 6, текущие права, которые хранятся в приемнике/декодере, сравниваются с предыдущими правами с помощью

избыточной информации о дате в виде контрольной даты 3110. Следовательно, собственно EMM 3062 содержит контрольную дату 3110, в дополнение к дате прав (или дате исчерпания прав) 3112, которая представляет собой дату, до которой будут действительны новые права, содержащиеся в EMM. Контрольная дата на один месяц (или иной подходящий период) меньше, чем дата прав. Собственно EMM также содержит сами права, в виде одного или обычно более ключей ECM 3114; предоставляется по крайней мере один ключ ECM для текущего месяца, так же - в предпочтительной реализации - как и ключ ECM для следующего месяца.

На фиг. 6 показано также соответствующее содержимое электрически-стираемого ППЗУ 108 смарт-карты, изображенного на фиг. 2. Это содержимое представляет собой дату прав 3116, записанную в смарт-карте.

Способ обработки группового EMM восстановления описывается с использованием блок-схемы, приведенной на фиг. 7. На первом шаге 3200 EMM принимается приемником/декодером 2020 и соответствующие данные передаются смарт-карте, которая вставлена в приемник/декодер и в данной ситуации рассматривается как часть приемника/декодера. EMM обрабатывается микропроцессором 100 смарт-карты и устройствами памяти 104, 106 и 108. На втором шаге 3202 битовый массив подписчиков 3100 проверяется в отношении данного подписчика. Если в соответствующем месте массива находится "1", микропроцессор обрабатывает EMM дальше, если в соответствующем месте находится "0", обработка прекращается. На третьем шаге 3204 записанная дата прав 3116 сравнивается с контрольной датой 3110. Если проверочная дата меньше или равна записанной дате прав, обработка продолжается; в противном случае обработка прекращается. На четвертом и последнем шаге 3206 записанная дата прав 3116 изменяется под управлением микропроцессора на новую

вещаемую дату прав 3112. Вещаемые ключи ECM 3114 могут затем быть использованы должным образом.

Возвращаясь к фиг. 6, проследим работу первого предпочтительного варианта реализации на примере с использованием трех строк, соответствующих январю, февралю и марту 1998 г. Во-первых, следует отметить, что вещание EMM восстановления группы производится несколько раз в течение соответствующего месяца. Для декабря 1997 электрически-стираемое ППЗУ 108 смарт-карты будет содержать дату прав 31.01.98, так что может использоваться соответствующий ключ ECM для декабря. Для января, в предположении, что вещание ключа ECM для января (следующего месяца) производится с EMM для декабря и дата прав равна 31.01.98, подписчик будет продолжать обладать правами даже до того, как EMM для января будет успешно принято. При первом успешном приеме EMM для января, поскольку контрольная дата 31.01.98 не больше, чем записанная дата прав 31.01.98, записанная дата прав заменяется на новую вещаемую дату прав 3112, которой является 28.02.98. При последующем приеме в январе EMM для января, выполняются шаги от 3200 до 3206, как показано на фиг. 7, но изменение записанной даты прав не производится.

В феврале, если, с одной стороны, подписчик № 3 оставил свой приемник/декодер 2020 включенным, февральское EMM будет принято и передано в смарт-карту, но поскольку (на шаге 3202, фиг. 7) значение для соответствующего места в битовом массиве равно "0", никакого изменения записанной даты прав не происходит и она остается равной 28.02.98. С другой стороны, если приемник/декодер 2020 оставили выключенным, сохраненная дата прав точно так же изменена не будет, хотя (как будет показано ниже) и по несколько иной причине.

В марте, независимо от того, чему сейчас равно значение в

соответствующем месте битового массива - "1" или "0", - записанная дата прав опять останется без изменений, поскольку контрольная дата 31.03.98 больше, чем записанная дата прав 28.02.98, и, следовательно, подписчик не получит ключ ECM, который можно использовать в марте. Его права, таким образом, будут эффективным образом аннулированы. Фактически, права могут быть перепредоставлены только с помощью специального EMM повторной активации.

Во втором предпочтительном варианте реализации, который может рассматриваться как особенно близкий к первому предпочтительному варианту реализации, контрольная дата 3110 в вещаемом EMM заменяется ключом ECM предыдущего месяца, и записанная дата прав 3116 заменяется ключом ECM текущего месяца (в противоположность ключу следующего месяца). Следовательно, вещание ключа ECM последнего месяца производится в сообщении текущего месяца. Выполняется сравнение либо самих ключей ECM, либо дат, соответствующих (и вещаемых с) ключами ECM. В обоих случаях вещаемый ключ ECM рассматривается как избыточная информация о дате, поскольку сам ключ ECM соответствует конкретному месяцу.

Таким образом, согласно фиг. 5, перед первым приемом январского EMM (которое будет содержать декабрьский ключ ECM в качестве избыточной информации о дате) в смарт-карте будет записан декабрьский ключ ECM. Результат сравнения вещаемого и записанного значения ключей ECM будет положительным, и, следовательно, декабрьский ключ ECM будет заменен январским ключом ECM.

Если несанкционированный подписчик отключит декодер в феврале, последние принятые права будут январскими. При появлении EMM для марта декодер обнаружит отсутствие ключа ECM за февраль и предпримет соответствующе действия, например, сообщит системе о проблеме

санкционирования, откажется передать права на март и т.д.

Первые два предпочтительных варианта реализации особенно предпочтительны, поскольку они используют в качестве записываемой в смарт-карту информации такую информацию, которая обычно в любом случае в нее сохраняется. Этим обеспечивает экономное использование пространства памяти смарт-карты.

В третьем предпочтительном варианте реализации избыточная информация о дате сохраняется в смарт-карту более чем за один предшествующий месяц. Например, так же как сохраняется информация за непосредственно предшествующий месяц, она может сохраняться за, положим, один или два предшествующих месяцев.

В четвертой предпочтительной реализации контрольная дата 3110 может быть заменена любыми подходящими контрольными данными 3110 (например, совершенно другой, возможно, случайной, контрольной датой, или другим случайным числом), и они, соответственно, могли бы быть сохранены в смарт-карту вместо сохраненной даты прав 3116. В таком случае дополнительно к дате прав 3112 может производиться вещание дополнительных контрольных данных, и возможно, что эти данные, а не дата прав 3112, может быть записана в смарт-карту для сравнения в следующем месяце с контрольными данными 3110.

В пятом предпочтительном варианте реализации вещание избыточной информации о дате не производится; вместо этого в смарт-карте или приемнике/декодере ведется учет того, было ли получено ежемесячное EMM. Если EMM за предшествующий месяц не принято, тогда, как в описанном выше первом варианте реализации, дальнейшая обработка EMM текущего месяца прекращается. Запись может быть, например, в форме таблицы. Таблица могла бы содержать EMM или ECM каждого месяца или его часть.

Как вариант описанного выше, если все подписчики правильно оплатили свою подписку, может оказаться не нужным пересылать с ЕММ битовый массив подписчиков, поскольку сообщение будет состоять целиком из положительных значений 1. Для упрощения битовый массив может пересылаться только при изменении подписчиков, как показано на фиг. 8.

Очевидно, что настоящее изобретение было описано выше исключительно в виде примера, и возможны различные модификации в пределах данного изобретения.

ИЗМЕНЕННАЯ ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, включающий операцию программирования приемника/декодера таким образом, что прием текущего EMM текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее EMM предыдущего календарного периода.

2. Способ по п. 1, дополнительно включающий следующие операции:

передача с текущим EMM избыточной информации о дате, и

прием текущего EMM и использование избыточной информации о дате для проверки факта приема упомянутого предыдущего EMM.

3. Способ по п. 2, в котором каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, и соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, причем указанная информация о контрольной дате представляет собой указанную избыточную информацию о дате.

4. Способ по пп. 2 или 3, в котором избыточная информация о дате представляет собой ключ сообщения управления правами (ключ ECM) предыдущего календарного периода.

5. Способ по пп. 2-4, в котором права подписчика изменяются через регулярные промежутки времени, и избыточная информация о дате относится к непосредственно предшествующему периоду.

6. Способ по любому из предшествующих пунктов, в котором календарные периоды не являются смежными во времени и/или эти периоды разделены нестандартизированными интервалами времени.

7. Способ по любому из предшествующих пунктов, в котором текущее ЕММ содержит битовый массив подписки, позиции которого представляют права подписки подписчиков в группе, факультативно, только при изменении прав подписчика.

8. Передатчик для использования в способе предотвращения несанкционированного доступа в системе условного доступа, подключенной к приемнику/декодеру подписчика чтобы принимать сообщения управления предоставлением прав (ЕММ) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, которым предусмотрено программирование приемника/декодера таким образом, что прием текущего ЕММ текущего календарного периода осуществляется только в том случае, когда им был принято по меньшей мере одно предыдущее ЕММ предыдущего календарного периода, где указанный передатчик содержит средства передачи с текущим ЕММ текущего календарного периода избыточной информации о дате, которая может быть использована приемником/декодером для проверки факта приема упомянутого предыдущего ЕММ.

9. Передатчик по п. 8, в котором каждое ЕММ содержит информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой указанную избыточную информацию о дате.

10. Передатчик по пп. 8 или 9, в котором избыточная информация о дате представляет собой ключ сообщения управления правами (ключ ECM)

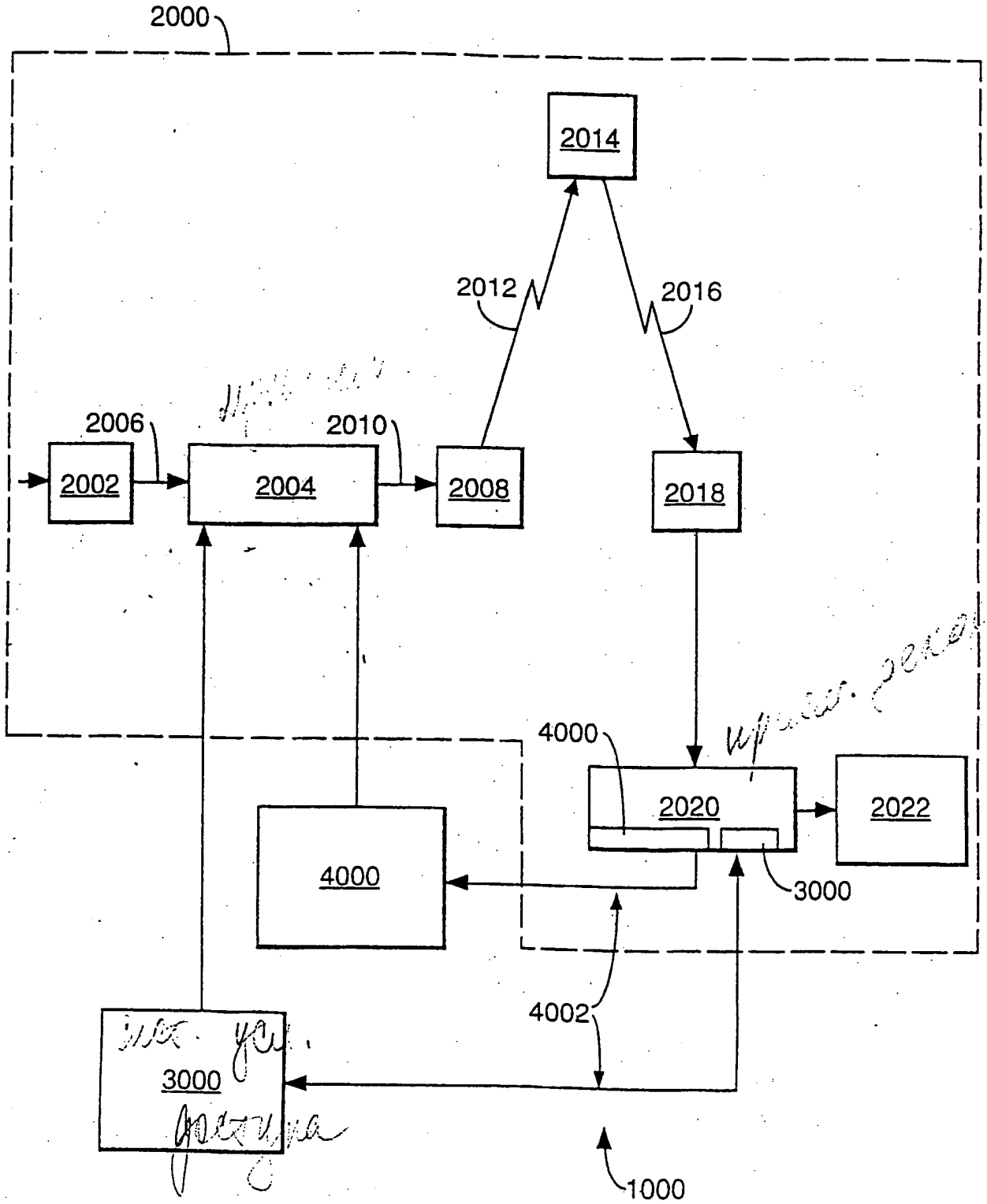
11. Приемник/декодер для использования в способе предотвращения несанкционированного доступа в системе условного доступа, который подключен к системе условного доступа и выполнен с возможностью приема сообщения управления предоставлением прав (EMM) для группы подписчиков, для предоставления упомянутой системе возможности предоставлять доступ соответствующему подписчику, содержащий средство, запрограммированное таким образом, чтобы осуществлять прием текущего EMM текущего календарного периода только в том случае, когда им было принято по меньшей мере одно предыдущее EMM предыдущего календарного периода.

12. Приемник/декодер по п. 11, в котором упомянутые средства запрограммированы для выполнения проверки факта приема предыдущего EMM, используя избыточную информацию о дате, содержащуюся в текущем EMM.

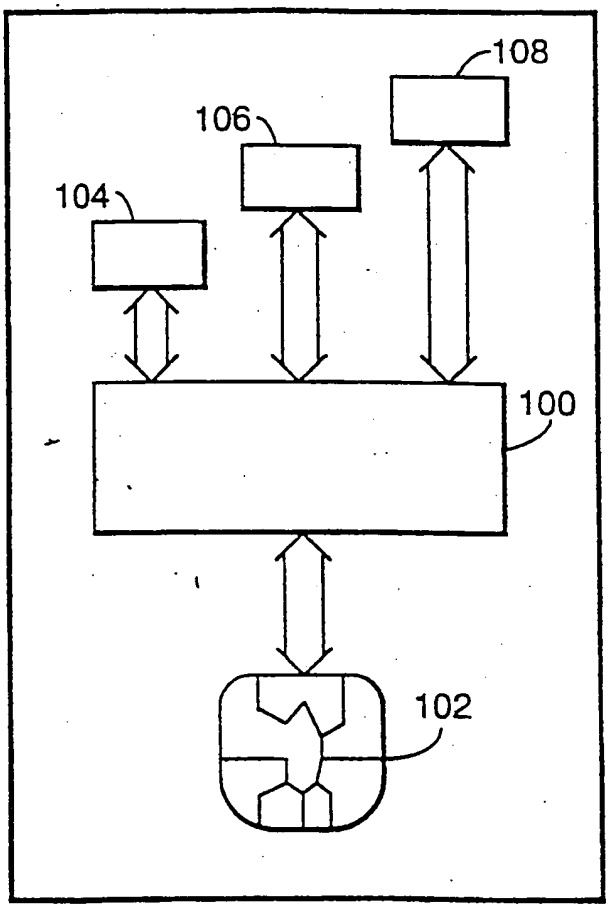
13. Приемник/декодер по п. 12, в котором каждое EMM содержит информацию о дате прав, касающуюся текущего права доступа, а также соответствующую информацию о контрольной дате, касающуюся предыдущего права доступа, которая представляет собой указанную избыточную информацию о дате.

14. Приемник/декодер по пп. 12 или 13, в котором избыточная информация о дате представляет собой ключ сообщения управления правами (ключ ECM) предыдущего календарного периода.

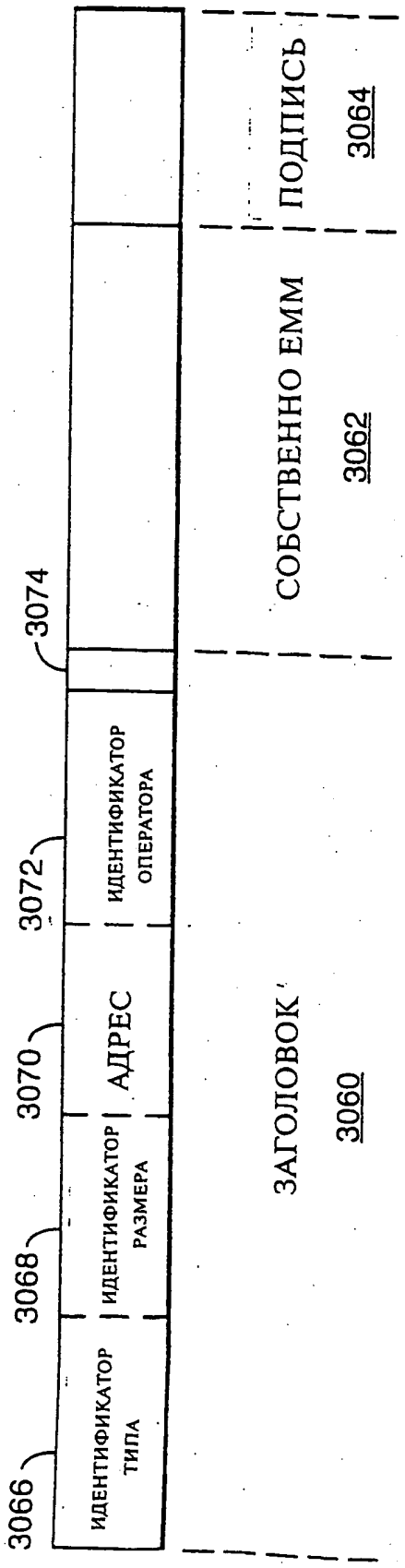
ФИГ. 1


2000
2014
2012
2016
2006
2010
2002
2004
2008
2018
4000
2020
2022
4000
3000
4002
3000
1000

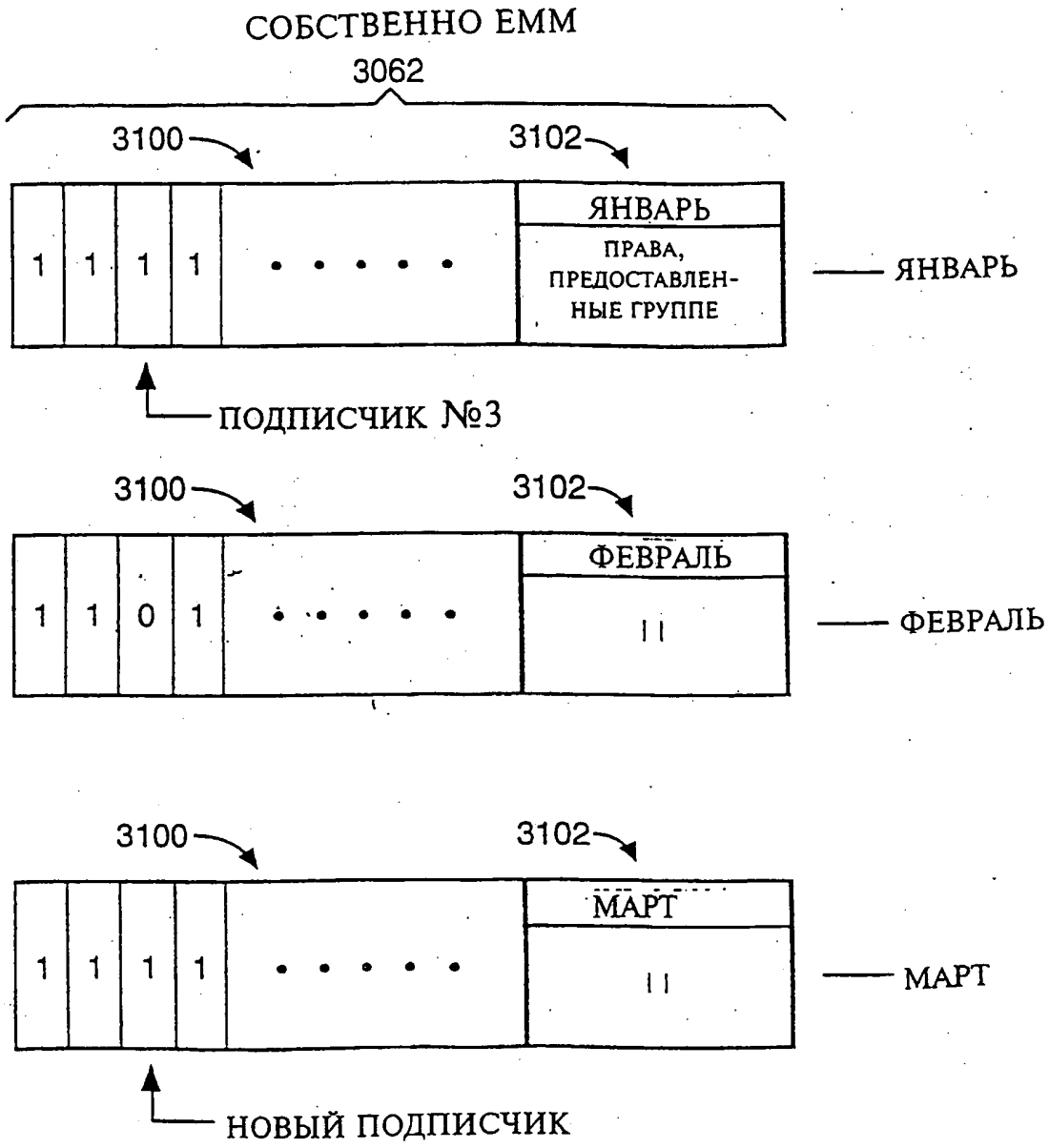
ФИГ. 2



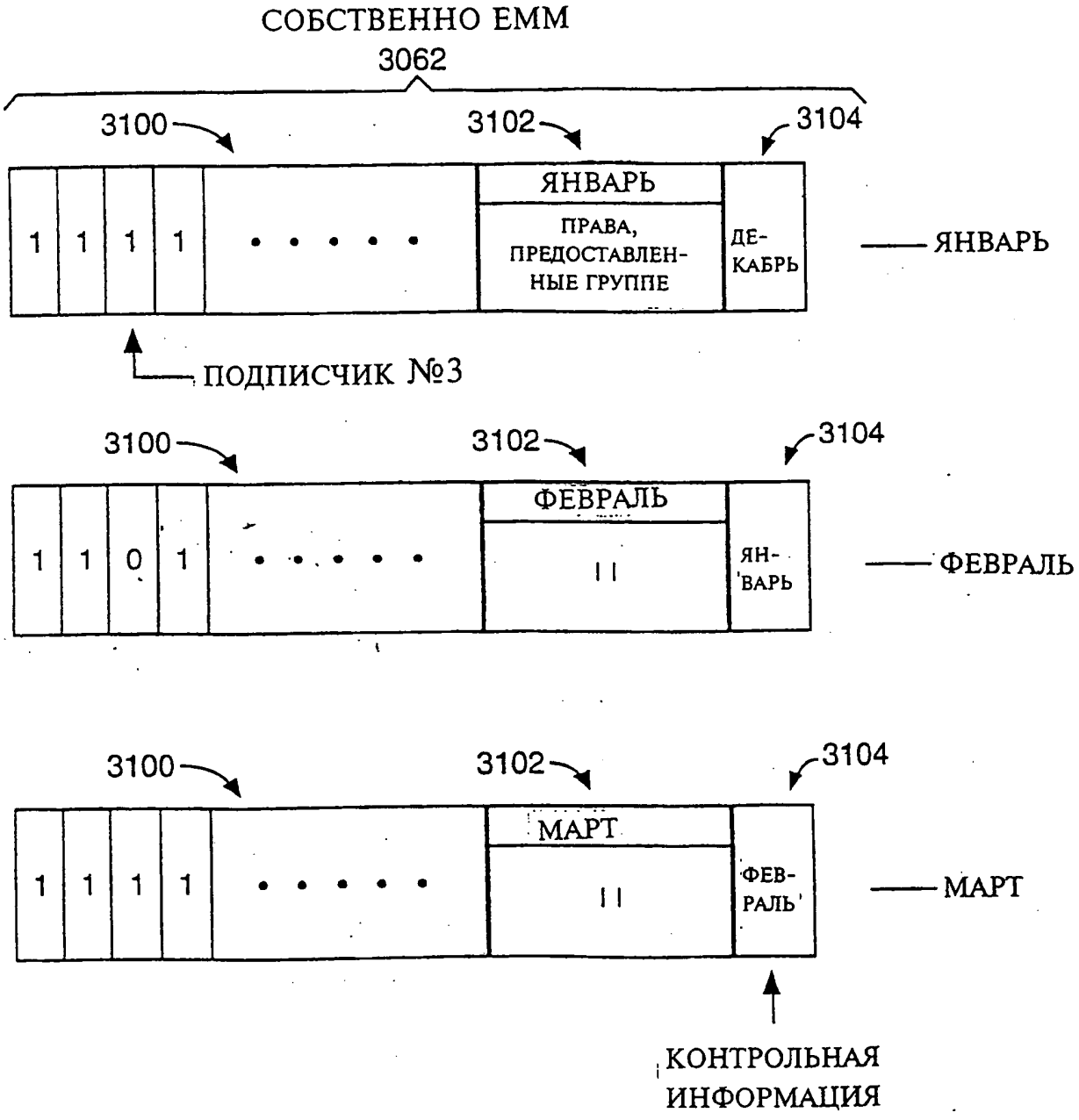
ФИГ. 3


3066
ИДЕНТИФИКАТОР ТИПА
3068
ИДЕНТИФИКАТОР РАЗМЕРА
3070
АДРЕС
3072
ИДЕНТИФИКАТОР ОПЕРАТОРА
3074
ЗАГОЛОВОК
3060
СОБСТВЕННО ЕММ
3062
ПОДПИСЬ
3064

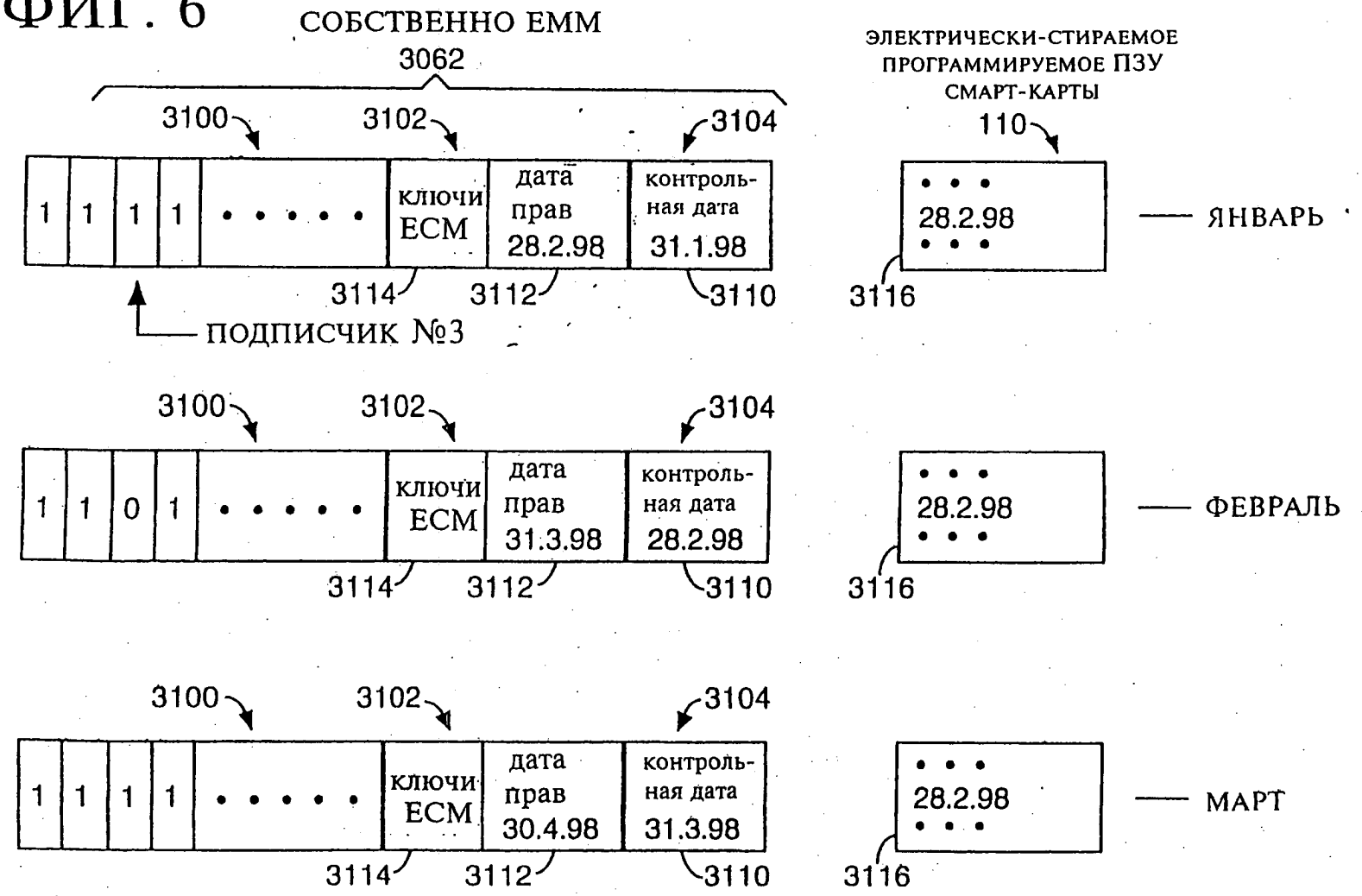
ФИГ. 4


СОБСТВЕННО ЕММ
3062
3100
3102
1 1 1 1 • • • • •
ЯНВАРЬ
ПРАВА, ПРЕДОСТАВЛЕННЫЕ ГРУППЕ
ЯНВАРЬ
ПОДПИСЧИК №3
3100
3102
1 1 0 1 • • • • •
ФЕВРАЛЬ
| |
ФЕВРАЛЬ
3100
3102
1 1 1 1 • • • • •
МАРТ
| |
МАРТ
НОВЫЙ ПОДПИСЧИК

ФИГ. 5

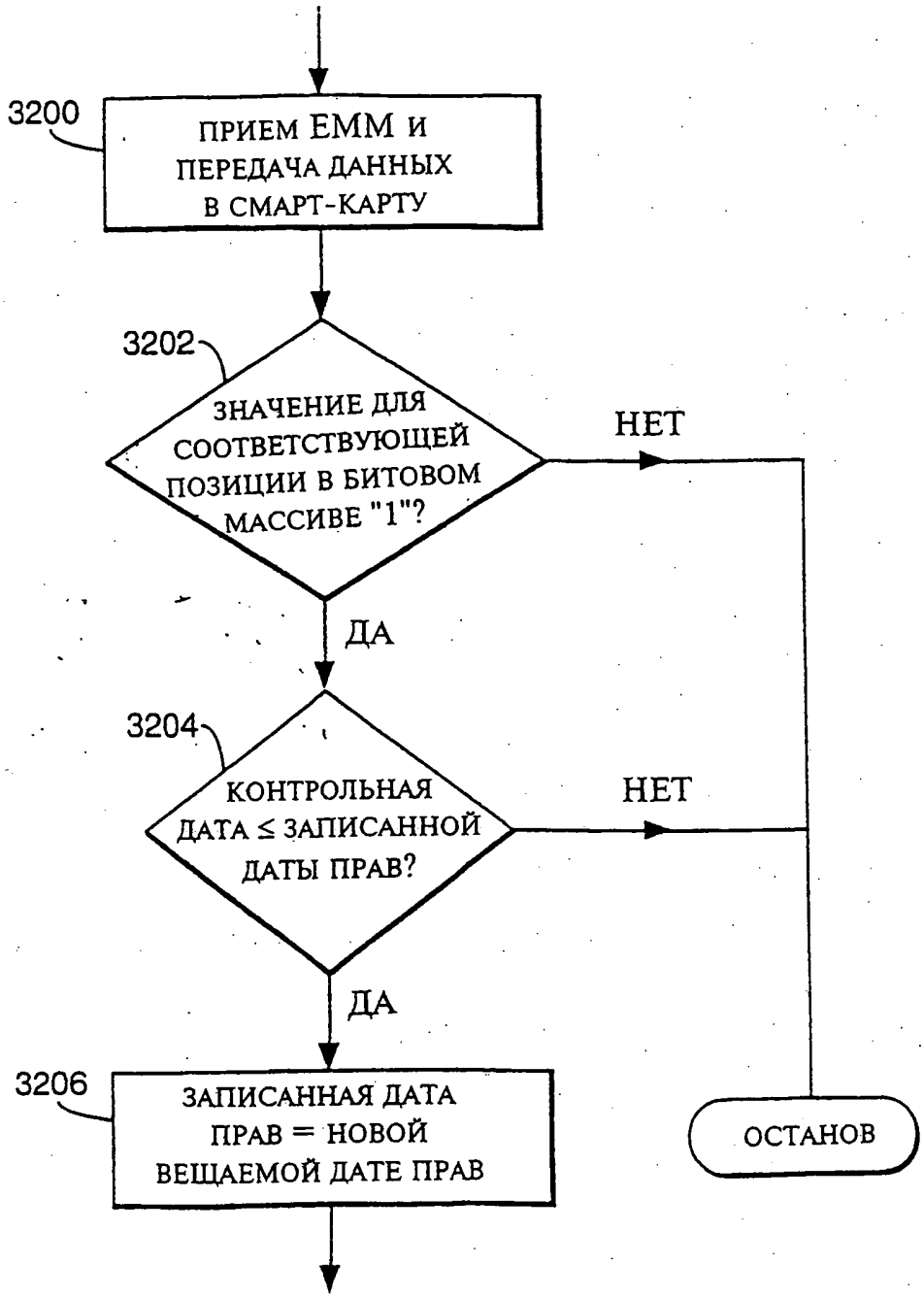

СОБСТВЕННО ЕММ
3062
3100
3102
3104
1 1 1 1 • • • • •
ЯНВАРЬ
ПРАВА, ПРЕДОСТАВЛЕННЫЕ ГРУППЕ
ДЕКАБРЬ
ЯНВАРЬ
ПОДПИСЧИК №3
3100
3102
3104
1 1 0 1 • • • • •
ФЕВРАЛЬ
| |
ЯНВАРЬ
ФЕВРАЛЬ
3100
3102
3104
1 1 1 1 • • • • •
МАРТ
| |
ФЕВРАЛЬ
МАРТ
КОНТРОЛЬНАЯ ИНФОРМАЦИЯ

ФИГ. 6

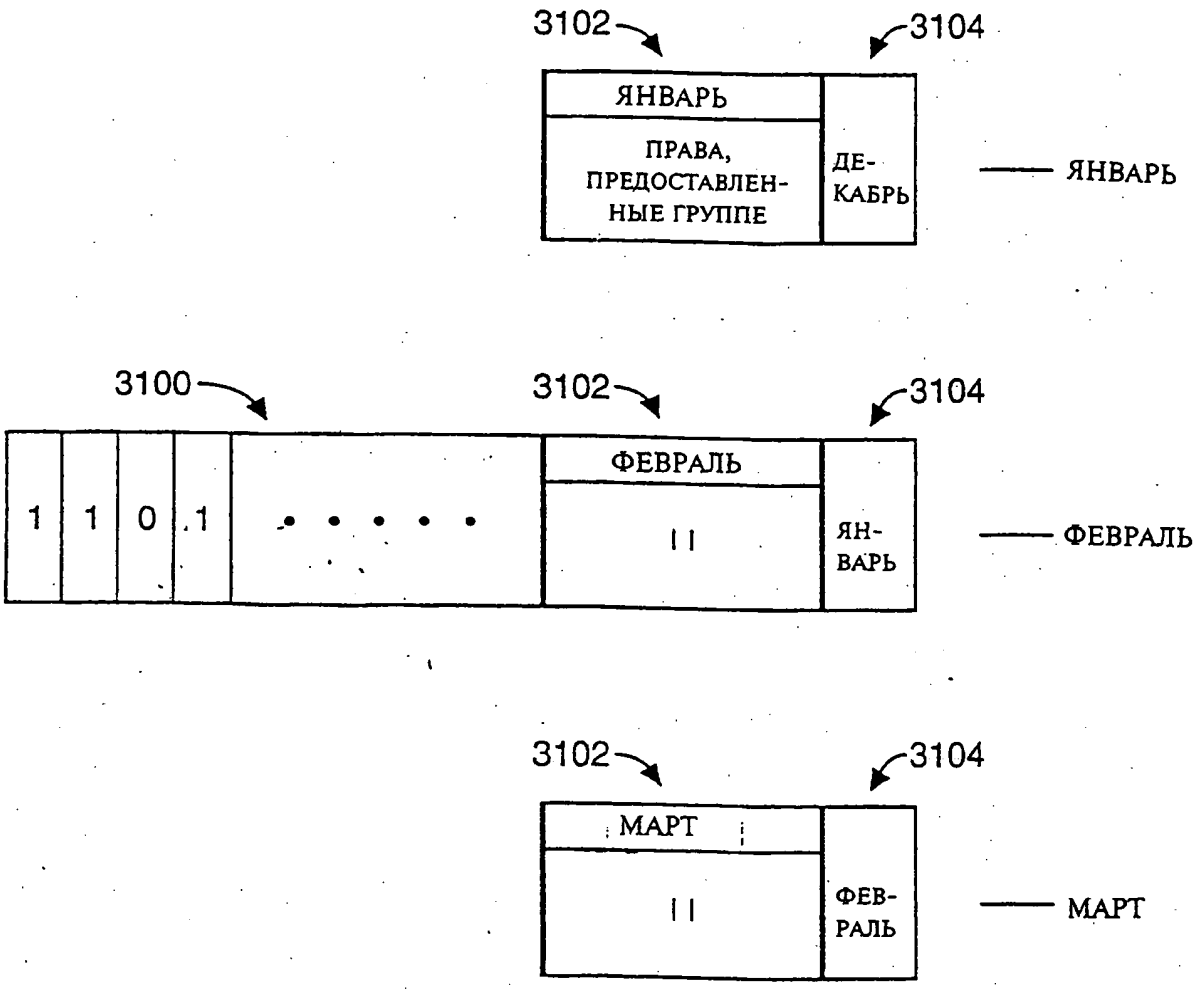


доступа в системе условного доступа

ФИГ. 7


3200
ПРИЕМ EMM И ПЕРЕДАЧА ДАННЫХ В СМАРТ-КАРТУ
3202
ЗНАЧЕНИЕ ДЛЯ СООТВЕТСТВУЮЩЕЙ ПОЗИЦИИ В БИТОВОМ МАССИВЕ "1"?
НЕТ
ДА
3204
КОНТРОЛЬНАЯ ДАТА ≤ ЗАПИСАННОЙ ДАТЫ ПРАВ?
НЕТ
ДА
3206
ЗАПИСАННАЯ ДАТА ПРАВ = НОВОЙ ВЕЩАЕМОЙ ДАТЕ ПРАВ
ОСТАНОВ

ФИГ. 8

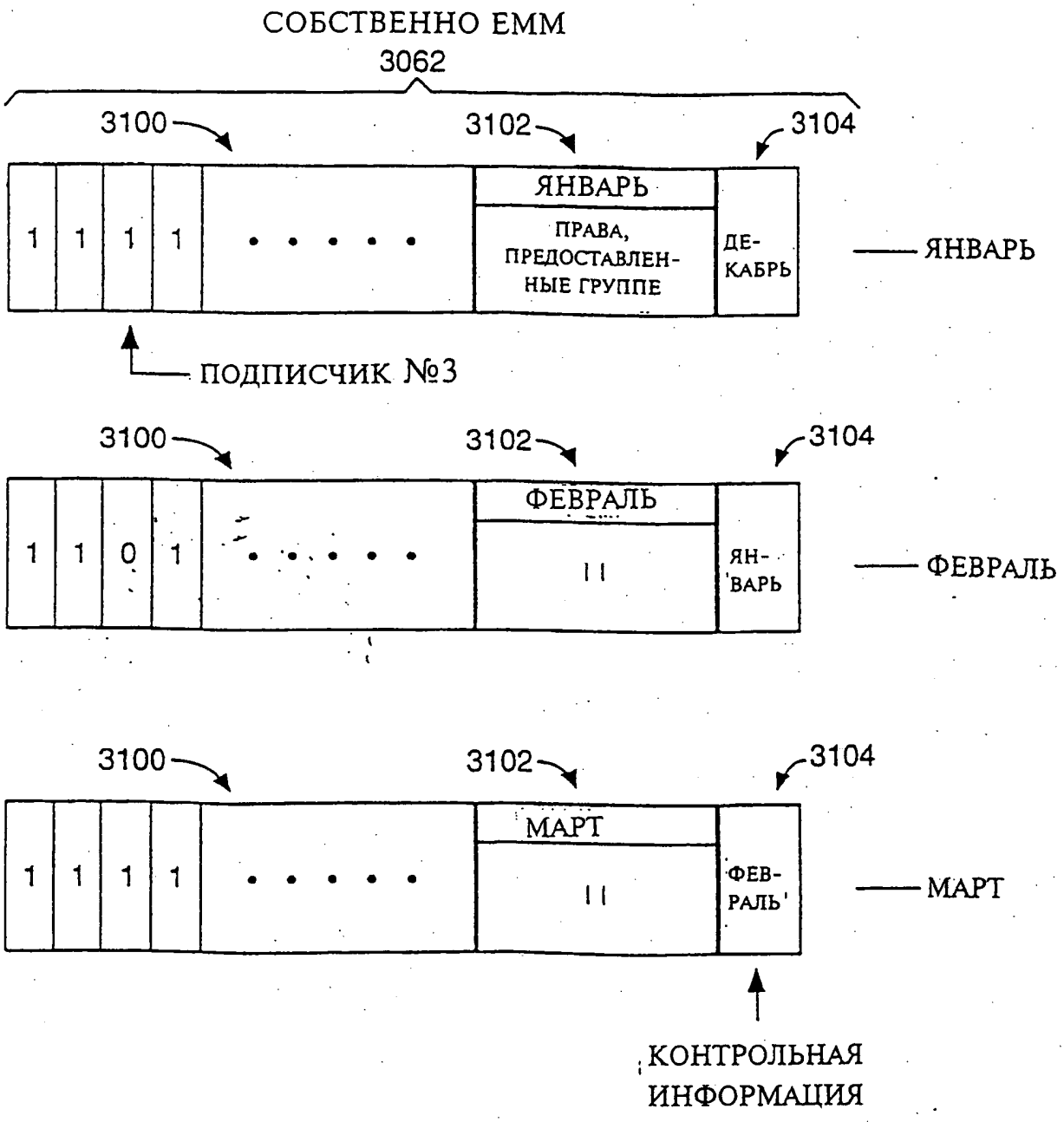

3102
3104
ЯНВАРЬ
ПРАВА, ПРЕДОСТАВЛЕННЫЕ ГРУППЕ
ДЕКАБРЬ
ЯНВАРЬ
3100
3102
3104
1 1 0 1
ФЕВРАЛЬ
ЯНВАРЬ
ФЕВРАЛЬ
3102
3104
МАРТ
ФЕВРАЛЬ
МАРТ

РЕФЕРАТ

Приемник/декодер программируется принимать текущее сообщение управления предоставлением прав (EMM) только тогда, если он принял по меньшей мере одно предыдущее EMM предшествующего календарного периода. После того, как оно принято, оно используется для проверки текущих прав в приемнике/декодере. Настоящее изобретение препятствует первоначальному подписчику в несанкционированном получении прав путем отключения декодера (до того, как сообщение санкционирования может обновить память декодера с целью воспрепятствовать дешифровке) и затем повторного включения декодера (так, что он оказывается перепутанным с новым подписчиком, получившим эти права законным образом).

Фиг. 5

ФИГ. 5


СОБСТВЕННО ЕММ
3062
3100
3102
3104
1 1 1 1 . . . . .
ЯНВАРЬ
ПРАВА, ПРЕДОСТАВЛЕННЫЕ ГРУППЕ
ДЕКАБРЬ
ЯНВАРЬ
ПОДПИСЧИК №3
3100
3102
3104
1 1 0 1 . . . . .
ФЕВРАЛЬ
| |
ЯНВАРЬ
ФЕВРАЛЬ
3100
3102
3104
1 1 1 1 . . . . .
МАРТ
| |
ФЕВРАЛЬ
МАРТ
КОНТРОЛЬНАЯ ИНФОРМАЦИЯ